CLASSIFYING GROUPS WITH SMALL SQUARING PROPERTIES

TERRY EDDY

Classifying groups with small squaring properties

by

Terry Eddy

A thesis submitted to the

School of Graduate Studies

in partial fulfillment of the

requirements for the degree of

Master of Science

Mathematics

Memorial University of Newfoundland

October 2006

St. John's, Newfoundland

Your file Votre référence
ISBN: 978-0-494-30464-8
Our file Notre référence
ISBN: 978-0-494-30464-8

Abstract

A group G is said to be a $B(n,k)$ group if $|A^2| \leq k$ for any n-subset A of G. The $B(2,3)$ groups were previously classified by Freiman and the $B(3,6)$ groups were classified by Parmenter. In addition, the $B(3,8)$ groups were partially classified by Berkovich, Freiman and Praeger, and their work was later completed by Longobardi and Maj. In this thesis, we will classify the $B(2,k)$ and $B(3,k)$ groups for all other values of k (except $B(3,7)$ where partial results are obtained). We will also provide some results for higher values of n, including the classification of the $B(4,10)$ groups by Parmenter and some classifications for a general value of n by Berkovich and also Herzog, Longobardi and Maj.

Acknowledgments

I would like to take this opportunity to acknowledge the following people who made the completion of this thesis possible. First, I would like to thank my parents for their unwavering support in everything that I do. Next, I thank my classmates, especially Jared Howell, for their suggestions and typesetting advice. I would also like to recognize the Department of Mathematics and Statistics at Memorial University of Newfoundland for funding this thesis and the rest of my graduate studies. Finally, and most importantly, I offer my deepest appreciation to my supervisor Dr. Michael Parmenter for all his help and support, and above all, his patience.

Contents

Chapter 1

Introduction

The problem we are considering concerns the structure of groups that satisfy certain conditions on the number of distinct products that can be obtained when we multiply all elements of any given subset by one another. This notion was introduced by Freiman [4] in 1981 and the similar case for rings was investigated later by Bell and Klein [1] in 2001.

Definition 1.1 *A B_k-group is a group G which satisfies the condition that if $\{a_1, \ldots a_k\}$ is a k-subset of G, then $|\{a_i a_j | 1 \leq i, j \leq k\}| \leq \frac{k(k+1)}{2}$.*

We will sometimes use another notation to represent the "squaring" of subsets, as follows.

Definition 1.2 *If we have a k-subset $A = \{a_1, \ldots a_k\}$ of a group G, then we define A^2 to be the set such that $A^2 = \{a_i a_j | 1 \leq i, j \leq k\}$.*

Freiman's condition is of interest since all abelian groups are B_k-groups, a fact which we will quickly show here. Given an abelian group G and some subset $S = \{a_1, \ldots, a_k\}$, when we multiply the elements on both sides we know that $a_1a_2 = a_2a_1$, $a_1a_3 = a_3a_1$, and so on. It follows that we have at least $\frac{k(k-1)}{2} = \binom{k}{2}$ repeated products, by commutativity, since $\binom{k}{2}$ is the number of ways to choose two distinct elements from a k-subset. If we subtract these repetitions from the total products we get

$$k^2 - \frac{k(k-1)}{2} = \frac{k^2+k}{2} = \frac{k(k+1)}{2},$$

hence, all abelian groups are B_k-groups. So, armed with this fact, it was Freiman's intention to determine which nonabelian groups satisfied the same condition.

A more general condition was later introduced by Berkovich, Freiman, and Praeger [2] in 1991 and is as follows.

Definition 1.3 *A group G is said to have the small squaring property on k-sets if $|K^2| < k^2$ for all k-element subsets K of G.*

This situation is of interest because it examines a broader range of groups; the idea being to discover which groups will have at least one repeated product when we multiply in the usual way, or equivalently, to find which groups give fewer than the usual k^2 products.

Definitions 1.1 and 1.3 along with their respective bounds are the original notions in the area, however, there was really no connection made between the two in the past. In what follows, we have consolidated and extended these definitions to include any bound. The new definition is as follows.

Definition 1.4 *A group G is called a $B(n,k)$ group if $|\{a_i a_j | 1 \leq i,j \leq n\}| \leq k$, for any n-subset $S = \{a_1, \ldots a_n\}$ of G.*

Using this new definition, we see that a B_k-group is a $B(k, \frac{k(k+1)}{2})$ group, while a group with the small squaring property on k-sets is a $B(k, k^2 - 1)$ group.

Clearly a $B(n,k)$ group is also a $B(n,k+1)$ group, a $B(n,k+2)$ group and so on. However, when we classify $B(n,k)$ groups, we will not repeat them as $B(n,k+1)$ groups, or equivalently, each group will be listed only in a class for the smallest value of k for which the necessary conditions hold for that group.

It seems appropriate to give a practical example of what we mean when we say a group is $B(n,k)$. In particular, we will later show that C_6, the cyclic group of order 6, is a $B(3,5)$ group, so this means if we take any 3-subset of C_6 then we will get at most five distinct products. For example, if we take the subset $S = \{x, x^2, x^3\}$ we multiply each element by every other element on both sides, i.e: $x \cdot x = x^2$, $x \cdot x^2 = x^3$, $x \cdot x^3 = x^4$, $x^2 \cdot x = x^3$, $x^2 \cdot x^2 = x^4$, $x^2 \cdot x^3 = x^5$, $x^3 \cdot x = x^4$, $x^3 \cdot x^2 = x^5$, $x^3 \cdot x^3 = x^6 = 1$. So we have the 5 distinct products $1, x^2, x^3, x^4, x^5$. The order in which these products were calculated will be the order for multiplying the elements of any subset from here on.

Clearly any group G where $|G| \leq k$ will automatically be a $B(n,k)$ group for any n, hence we define the following:

Definition 1.5 *A nontrivial $B(n,k)$ group G is a $B(n,k)$ group where $|G| > k$.*

There are a collection of groups that will appear often, so they will be defined here for simplicity.

$Q_8 = \langle a, b | a^4 = 1, a^2 = b^2, ba = a^3 b \rangle$, the quaternion group of order 8.

$S_3 = \langle a, b | a^3 = 1, b^2 = 1, ba = a^2 b \rangle$, the permutation group of order 6.

$D_{2n} = \langle a, b | a^n = b^2 = 1, ba = a^{n-1} b \rangle$, the dihedral group of order $2n$.

We now define another important family of groups.

Definition 1.6 *A group H is called Hamiltonian if H is nonabelian and every subgroup of H is normal.*

We will be working frequently with the Hamiltonian groups. The following theorem regarding the structure of the Hamiltonian groups is a well known result in group theory and will be needed later. It appears here from Hall [5].

Theorem 1.1 *A group is Hamiltonian if and only if it is the direct product of a quaternion group with an abelian group in which every element is of finite odd order, and an abelian group of exponent two.*

Proof: $\Longrightarrow$

Let a and b be two elements of a Hamiltonian group H. Then the commutator $c = (a, b) = (a^{-1}b^{-1}a)b = b^s = a^{-1}(b^{-1}ab) = a^r$, since $\langle a \rangle$ and $\langle b \rangle$ are both normal subgroups. Note that this implies that c commutes with a and also with b. Then

$$(a^2, b) = (a, b)(c, a)(a, b) = (a, b)^2,$$

and we may prove similarly by induction that

$$(a^i, b) = (a, b)^i = c^i,$$

for all positive i. If a and b do not commute, then $c = a^r \neq 1$, and putting $i = r$ or $i = -r$, whichever is positive, we see that (a^i, b) is either (c, b) or (c^{-1}, b) and is the identity in either event since c commutes with b. We now have $(a^i, b) = 1 = (a, b)^i = c^i$, hence $c^i = 1$ and $a^{ri} = 1 = b^{si}$, which means that any noncentral element of H is of finite order. If an element x is central in H and a is noncentral, then xa is noncentral and it follows that xa, and so also x, is of finite order. It now follows that every element of H is of finite order.

Let a and b be elements of H which do not commute, and let $a^N = 1 = b^M$ where we suppose N and M are minimal (replacing a and b by suitable powers if necessary). If p is any prime divisor of N, then by the minimality of N, a^p commutes with b, and so, $(a^p, b) = (a, b)^p = 1$. The same will hold for any prime dividing M. As $c = (a, b) \neq 1$, there can be only one prime dividing M and N, and $|M| = p^m$, $|N| = p^n$. Thus $a^{p^n} = 1$, $b^{p^m} = 1$, $c = (a, b)$, $c^p = 1$, where, by symmetry, we may assume $n \geq m$. Further, since $c \in \langle a \rangle$ and $c \in \langle b \rangle$, we have that $c = a^{jp^{n-1}} = b^{kp^{m-1}}$, where $j, k \not\equiv 0 \ (mod\ p)$.

In $\langle a, b \rangle$ the derived group is $\langle c \rangle$ and is in its center. We now establish the formula

$$(ab)^i = a^i b^i (b, a)^{i(i-1)/2}$$

by induction. The result is clearly true for $i = 1$. For $i + 1$, we obtain

$$(ab)^{i+1} = (ab)^i ab = a^i b^i (b,a)^{i(i-1)/2} ab = a^i b^i ab (b,a)^{i(i-1)/2}$$

$$= a^i a b^i (b^i, a) b (b,a)^{i(i-1)/2} = a^{i+1} b^i (b,a)^i b (b,a)^{i(i-1)/2} = a^{i+1} b^{i+1} (b,a)^{i(i+1)/2}.$$

This proves the formula by induction for any group $\langle a, b\rangle$ in which (a, b) is in the center.

If $b_1 = a^u b^k$, where $u = -jp^{n-m}$, then $\langle a, b_1\rangle = \langle a, b\rangle$, whence b_1 does not commute with a, and therefore by assumption, the order of b_1 is at least as great as that of b. The formula just established yields

$$b_1^p = (a^u b^k)^p = a^{up} b^{kp} (b^k, a^u)^{p(p-1)/2} = a^{up} b^{kp} c^{-ukp(p-1)/2},$$

whence

$$b_1^{p^{m-1}} = a^{-jp^{n-1}} b^{kp^{m-1}} c^{jkp^{n-1}(p-1)/2} = c^{jkp^{n-1}(p^m-1)/2}.$$

Here $b_1^{p^{m-1}} \neq 1$, but since $c^p = 1$, we must have $p = 2 = n$. Thus the relations on a and b are $a^2 = b^2 = a^{-1}b^{-1}ab = c$, $c^2 = 1$, and $\langle a, b\rangle$ is the quaternion group. This shows that any nonabelian subgroup of H contains a quaternion group.

We know, because of the last paragraph, that H has a subgroup $Q = \langle a, b | a^4 = 1, a^2 = b^2, ba = a^3 b\rangle$ isomorphic to the quaternion group. We next show that H is the product of Q and the group Z of elements centralizing Q. If an element x of H does not commute with a, then $x^{-1}ax = a^{-1}$ and hence xb commutes with a. Similarly, if x (or xb) does not commute with b, then xa (or xba) commutes with b, and so one of the elements x, xb, xa, xba lies in Z. Hence $H = QZ$. We now show that Z

cannot contain an element of order 4. Suppose $x^4 = 1$, $x \in Z$, then $(a, bx) \neq 1$. But $(bx)^4 = 1$, so we have $a^{-1}(bx)a = (bx)^{-1}$, whence $a^{-1}bax = b^{-1}x^{-1}$, giving $x^2 = 1$. Since Z contains no element of order 4, it cannot contain a quaternion group, and it follows that Z is abelian. Because $Z \cap Q = \langle a^2 \rangle$, we can, by Zorn's lemma, find a subgroup Z_1 of Z maximal with respect to the property of not containing a^2. It now follows that $Z = Z_1 + Z_1 a^2$, and $H = Q \times Z_1$. We see that Z_1 is the direct product of the abelian group U, whose elements are of odd order, and an abelian group V of exponent 2 (since Z_1 contains no element of order 4) thus $H = Q \times U \times V$.

$\Longleftarrow$

To prove that $Q_8 \times U \times V$ is Hamiltonian, it suffices to show that every cyclic subgroup $\langle quv \rangle$ is normal. Since U and V are in the center of $Q_8 \times U \times V$, we need only show that a and b transform this group into itself. Clearly $a^{-1}(quv)a = q^i uv$, where $i = 1$ or 3, and since the order of u is an odd number n, the congruences $r \equiv i \ (mod\ 4)$, $r \equiv 1 \ (mod\ n)$ are solvable. Furthermore, since the order of v is 2, we conclude that $a^{-1}(quv)a = (quv)^r$. Clearly the same argument works for $b^{-1}(quv)b$, so the proof of the theorem is complete. □

For any other general group theory results which may be implicitly stated, see Rotman [9].

In this thesis, we provide a basis for the classifications of $B(n, k)$ groups for small values of n. In Chapter 2, we completely classify $B(2, k)$ groups. Next, Chapter 3 is the main chapter in the thesis in which we provide a near-complete classification

of the $B(3,k)$ groups. In Chapter 4, we show some results involving $B(4,k)$ groups, and make a start towards a complete classification. Finally, Chapter 5 is comprised of some interesting general results involving $B(n,k)$ groups, which hold for many (and sometimes all) values of n. For most of this thesis it will be assumed that all groups are finite (although some of the results can be extended to the general case). However, in Chapter 5 we do allow the possibility of G being infinite.

Chapter 2

$B(2,k)$ groups

The case of $B(2,k)$ groups serves as a nice starting point to illustrate the basics of small squaring. We begin with the first result in this area as shown by Freiman [4].

Theorem 2.1 *A group G is $B(2,3)$ if and only if G is either abelian or a Hamiltonion 2-group.*

Proof: $\Longleftarrow$

We take a subset $\{x,y\}$ where $x,y \in G$. If G is abelian, we have $xy = yx$, and thus there exists at most three distinct products. So we check the case where G is a Hamiltonion 2-group, i.e. $Q_8 \times C_2 \ldots \times C_2$. We may assume by the last remark that x and y do not commute. But since all elements of order 2 are central, then $x^2 = y^2$, and so there exist at most three distinct products. Consequently, the listed groups are $B(2,3)$.

$\Longrightarrow$

Assume G is a nonabelian $B(2,3)$ group. We recall that a Hamiltonian group is a group in which every subgroup is normal, and this holds if and only if for every $x, y \in G$, $y^{-1}xy = x^i$ for some i.

Consider the subset $\{x, y\}$, where $x, y \in G$ do not commute. Since G is a $B(2,3)$ group, this forces $x^2 = y^2$. Next, we consider the subset $\{x, xy\}$. Again, x and xy don't commute, so we get $x^2 = (xy)^2 = xyxy \Rightarrow x = yxy$ or $y^{-1}xy = xy^2 \Rightarrow y^{-1}xy = x^3$ since $y^2 = x^2$. So G is Hamiltonion, or equivalently, $G \cong Q_8 \times C_2 \times \ldots \times C_2 \times A$ where A is abelian and $|A|$ is odd by Theorem 1.1 above.

Note that $\{x, y^3\} = \{x, x^2y\}$. Since x and x^2y don't commute, $x^2 = (y^3)^2 = y^6 = x^6$, so $x^4 = 1$ for all noncentral $x \in G$. It follows that $|A| = 1$ and we're done. $\square$

Next we classify the $B(2,2)$ groups. This is the first case where we digress from the already investigated bounds of $|A^2|$ whereby $|A^2| \leq \frac{k(k+1)}{2}$ and $|A^2| < k^2$, for any k-subset $A \subseteq G$.

Theorem 2.2 *A group G is a $B(2,2)$ group if and only if $G \cong C_2 \times \ldots \times C_2$.*

Proof: $\Longleftarrow$

Consider a subset $\{x, y\}$ where $x, y \in G$, from which we get the products x^2, xy, yx, y^2. Clearly, $yx = xy$ and $x^2 = 1 = y^2$, so we can obtain only two distinct products. Therefore G is $B(2,2)$.

$\Longrightarrow$

Let G be a $B(2,2)$ group. If we consider the subset $\{1, x\}$, we obtain the products $1, x, x^2$, of which only two are distinct, hence, by the cancellation law, we must have $x^2 = 1$. It follows that every element of G must be of order 2. Consequently G is abelian and hence $G \cong C_2 \times \ldots \times C_2$, as required. $\square$

Chapter 3

$B(3,k)$ groups

To date, the case where $n = 3$ has been the most commonly investigated. Here, we have examined all possibilities and completed the cases for the "non-traditional" values of k which were not previously solved (except for the partial result provided for the $B(3,7)$ case, as previously mentioned). We begin this section, in a similar manner as the last, by detailing the $k = \frac{3(4)}{2} = 6$ case with a theorem from Parmenter [8].

Theorem 3.1 *There are no nontrivial, nonabelian $B(3,6)$ groups.*

Proof: Assume that G is a nonabelian $B(3,6)$ group. We first show that if x and y are two noncommuting elements of G, then $\langle x, y\rangle \cong S_3$. For this we investigate three cases:

• First, suppose that $x^2 = 1$ and $y^2 \neq 1$, and consider a subset $\{x, y, xy\}$. Multiplying in the usual way, we get the products $1, xy, y, yx, y^2, yxy, xyx, xy^2, xyxy$. Clearly

$1, xy, y, yx, y^2, yxy$ must be distinct, so $xyx, xy^2, xyxy$ must all be equal to an element from the list of distinct elements. Clearly, the only possibility for xy^2 is $xy^2 = yx$. The possibilities for $xyxy$ are $xyxy = 1, yx$ or y^2. But, since $xy^2 = yx$, $xyxy$ must be equal to 1, since $xyxy = yx \Rightarrow xyxy = xy^2 \Rightarrow x = 1$ is a contradiction, as is $xyxy = y^2 \Rightarrow x^2y^3 = y^2 \Rightarrow y = 1$. From these two conditions we then get $xyx = x^2y^2 = y^2$. But then $y^3 = y^2y = xyxy = 1$, and so $\langle x, y\rangle \cong S_3$ as required.

- In this case we assume $x^2 = 1 = y^2$ and we know that $(xy)^2 \neq 1$ since $xy \neq yx$. Since $\langle x, y\rangle = \langle x, xy\rangle$, we are covered by the previous case.

- Finally, we assume $x^2 \neq 1$ and $y^2 \neq 1$. We first consider a subset $\{1, x, y\}$ and multiplying we get the products $1, x, y, x^2, xy, yx, y^2$. Since the first six of these elements must be distinct we can conclude that $x^2 = y^2$ in this case. Next, consider the subset $\{x, y, xy\}$. Multiplying in the usual way, we obtain the products $x^2, xy, x^2y, yx, y^2, yxy, xyx, xy^2, xyxy$. Clearly $x^2, xy, x^2y, yx, yxy, xy^2$ must be distinct and $x^2 = y^2$ from above, so xyx and $xyxy$ must equal one of the six distinct elements. The only possibility for xyx is $xyx = yxy$, and the two possibilities for $xyxy$ are $xyxy = x^2$ or yx. However, $xyxy = x^2 \Rightarrow x^2yx = x^2 \Rightarrow yx = 1$ is a contradiction since $xy \neq yx$, and $xyxy = yx \Rightarrow x^2yx = yx \Rightarrow x^2 = 1$ contradicts our assumption above. Since both of these choices are incompatible with $xyx = yxy$, this case fails.

Next, we show that $G \cong S_3$ is a trivial $B(3,6)$ group. So let x and y be any two noncommuting elements of G. We wish to show that $\langle x, y\rangle = G$. Since we have already shown that $\langle x, y\rangle \cong S_3$, we may assume that $x^2 = 1 = y^3$ and $yx = xy^2$.

Assume that z is an element not in $\langle x, y\rangle$ and that x and z don't commute (otherwise we can replace z by yz). It now follows from the above that $\langle x, z\rangle \cong S_3$, and since we know that $x^2 = 1$, we must have either $z^3 = 1$ or $(xz)^3 = 1$. Replacing z by xz (similarly to before) if necessary, we may assume that $z^3 = 1$. But then if we choose the subset $\{x, y, z\}$ we get the seven distinct products $1, xy, xz, yx, y^2, yz, z^2$, which is a contradiction. So $G \cong S_3$, and since S_3 is a trivial $B(3, 6)$ group, the proof is complete. □

In a manner similar to the last chapter, we will work backwards for smaller values of k, and will now consider the cases $k = 3, 4, 5$. First, we must show that S_3 is not a $B(3, 5)$ group. To see this, take the subset $S = \{a, b, ab\}$ where a is of order 3 and b is of order 2. Multiplying in the usual way we get the six products $a^2, ab, a^2b, 1, b, a$, so S_3 cannot be $B(3, 5)$, as claimed. □

Hence, by Theorem 3.1 and the above remark, we may assume that G is abelian in the following cases where $k = 3, 4, 5$.

Theorem 3.2 *There are no nontrivial $B(3, 3)$ groups.*

Proof: Assume G is a nontrivial $B(3, 3)$ group. Taking a subset $\{1, x, y\}$, we get the products $1, x, y, x^2, xy, y^2$. Since only three of these are distinct, the products x^2, xy, y^2 must be equal to either 1, x or y. Using the cancellation law, we get $xy = 1$, and we are left with the possibilities $x^2 = 1$ or $x^2 = y$. But in the first case $x^2 = 1 = xy$ from

above, contradicting the cancellation law, so $x^2 = y$. This means that G can have only three elements, which is a contradiction. □

Theorem 3.3 *G is a nontrivial $B(3,4)$ group if and only if $G \cong C_2 \times \ldots \times C_2$.*

Proof: $\Longleftarrow$

If $G \cong C_2 \times \ldots \times C_2$, take any subset $\{x, y, z\}$. Since $x^2 = y^2 = z^2 = 1$, G is $B(3,4)$.

$\Longrightarrow$

Assume G is a nontrivial $B(3,4)$ group and x is of order greater than 2. Taking the subset $\{1, x, x^2\}$, we get the products $1, x, x^2, x^3, x^4$. Since these products cannot be distinct, x must be of order ≤ 4.

Now, since G is a nontrivial $B(3,4)$ group it must also contain an element y such that y is not in $\langle x \rangle$. If we consider the subset $\{1, x, y\}$, we get the products 1, x, y, x^2, xy, y^2. However, 1, x, y, x^2, and xy are all distinct, which is a contradiction. Therefore no such x exists, and $G \cong C_2 \times \ldots \times C_2$ as desired. □

Theorem 3.4 *G is a nontrivial $B(3,5)$ group if and only if $G \cong C_6$ or $G \cong C_4 \times C_2 \times \ldots \times C_2$.*

Proof: $\Longleftarrow$

If $G \cong C_6 = \langle x \rangle$, we consider a subset $\{x^a, x^b, x^c\}$. Multiplying, we get the products $x^{2a}, x^{a+b}, x^{a+c}, x^{2b}, x^{b+c}, x^{2c}$, whereby the sum of these exponents is $4a + 4b + 4c$. However, the sum of the exponents of the set $x^0, x^1, x^2, x^3, x^4, x^5$ is 15, but

since $4a + 4b + 4c \neq 15(mod\ 6)$, our list of products cannot produce all powers of x. Therefore we have at most five distinct powers of x present, so C_6 is $B(3,5)$ as required.

If $G \cong C_4 \times C_2 \times \ldots \times C_2$ we know that either $x^2 = 1$ or x^2 is the element $(a^2, 1, \ldots, 1)$ of order 2. So if we take a subset $\{x, y, z\}$, then two of x^2, y^2, z^2 must be equal, and consquently, $G \cong C_4 \times C_2 \times \ldots \times C_2$ is $B(3,5)$.

$\Longrightarrow$

We next assume that G is $B(3,5)$. Since $C_2 \times \ldots \times C_2$ is $B(3,4)$, we may assume that x is of order greater than 3. Next, we wish to show that the order of x is strictly less than 6. If we consider the subset $S = \{1, x, x^3\}$ then, multiplying in the usual way, we get the products $1, x, x^3, x^2, x^4, x^6$. Since these elements cannot all be distinct, we know that every element has order at most 6. It is necessary, therefore, to consider only the groups $C_4 \times \ldots \times C_4 \times C_2 \times \ldots \times C_2$, $C_3 \times \ldots \times C_3 \times C_2 \times \ldots \times C_2$, and $C_5 \times \ldots \times C_5$.

Assume first that we can take the subset $\{x, y, xy\}$, where x, y are generators of different C_k's, with $k > 2$. From here we get the products $x^2, xy, x^2y, y^2, xy^2, x^2y^2$, which are all distinct and so we cannot have more than one such C_k. Clearly C_3, C_4, C_5, and $C_2 \times \cdots \times C_2$ are $B(3,5)$ groups (the first three being trivial $B(3,5)$ groups), so either $G \cong C_4 \times C_2 \times \ldots \times C_2$ or $G \cong C_3 \times C_2 \times \ldots \times C_2$, with at least one C_2 term. To finish we must investigate the latter.

We let $G \cong C_3 \times C_2 \times \ldots \times C_2$ with at least two copies of C_2, and take the subset $\{1, xy, x^2z\}$ where $x \in C_3$ and y, z are generators of different C_2's. But since the products $1, xy, x^2z, x^2, yz, x$ are clearly all distinct, we cannot have more than one C_2. Therefore we can have only $C_3 \times C_2 \cong C_6$ in this case, and we're done. $\square$

Next we will state a result from Berkovich, Freiman and Praeger [2] which partially classifies $B(3,8)$ groups. This was the original theorem classifying groups with the "small squaring property".

Theorem 3.5 *If G is a $B(3,8)$ group, then one of the following is true:*

(i) G is abelian.

(ii) G is a nonabelian 2-group.

(iii) $G = TP$, where T is a nontrivial normal abelian odd order subgroup and P is a nontrivial 2-group. Furthermore, the subgroup Q of P which centralises T has index 2 in P and each element of $P - Q$ inverts T. Thus we must have either (a) P is abelian and Q is elementary abelian, or (b) P is nonabelian, Q is abelian, and each element of $P - Q$ inverts Q.

Conversely any group satisfying (i) or (iii) is a $B(3,8)$ group.

The proof of Theorem 3.5 will be omitted. Instead we will establish a somewhat analagous result for the previously unexamined case of $B(3,7)$ groups. The proof of this theorem will occupy the next 13 pages.

Theorem 3.6 *If G is a nontrivial, nonabelian $B(3,7)$ group, then either G is a 2-group or $G = \langle p, t | p^4 = 1, t^3 = 1, pt = t^2p \rangle$. Conversely, the latter group is $B(3,7)$.*

Proof: First we will show that $G = \langle p, t | p^4 = 1, t^3 = 1, pt = t^2p \rangle$ is a $B(3,7)$ group. To simplify the proof, we rewrite G as $G = \langle a, p | a^6 = 1, a^3 = p^2, pa = a^5p \rangle$ by setting $a = p^2t$ and leaving p as before. We note that $A = \{1, a, a^2, a^3, a^4, a^5\}$ is a cyclic subgroup of G, and the set of elements $H = \{p, ap, \ldots, a^5p\}$ all have the same square, namely a^3. We also see that in this group there are six elements of order 4 (the set H), two elements each of orders 3 and 6, one element of order 2, and the identity. We proceed by taking a subset $\{x, y, z\}$ and investigating the different possibilities of the orders of x, y and z in an effort to find at least two repetitions of products in each case. Note that if any of x, y, z are of order at most 2, then such an element would be central and would automatically give two repetitions. So next we assume that any of x, y, z are of order at least 3 and consider the following cases.

(*i*) $|x| = 3$, $|y| = 6$, $|z| = 3$ or $|x| = 3$, $|y| = 6$, $|z| = 6$

Since all of these elements are contained in the cyclic subgroup A mentioned above, x, y, z will commute with each other, immediately giving at least 2 repetitions, i.e. $xy = yx$ and $xz = zx$.

(*ii*) $|x| = 3$, $|y| = 4$, $|z| = 6$

We take the subset $\{a^i, a^j, a^kp\}$ where $i = 1$ or 5, $j = 2$ or 4, $0 \leq k \leq 5$, which gives the products $a^{2i}, a^{i+j}, a^{i+k}p, a^{i+j}, a^{2j}, a^{j+k}p, a^{k-i}p, a^{k-j}p, a^3$. We already have the product a^{i+j} repeated once, so we need only find one more repetition. We examine all possible

values of i and j.

i	j	resulting repetition
1	2	$a^3 = a^{i+j}$
1	4	$a^{2i} = a^{2j}$
5	2	$a^{2i} = a^{2j}$
5	4	$a^{i+j} = a^3$

We have found a repetition for all possible values of i and j, so we have the required two repetitions for this case.

(iii) $|x| = 3$, $|y| = 3$, $|z| = 4$

This is the subset $\{a^2, a^4, a^i p\}$ where $0 \leq i \leq 5$, which gives the products $a^4, 1, a^{i+2}p, 1, a^2, a^{i+4}p, a^{i+4}p, a^{i+2}p, a^3$. Clearly 1, $a^{i+4}p$ and $a^{i+2}p$ appear twice, so this case holds.

(iv) $|x| = 6$, $|y| = 6$, $|z| = 4$

This is the subset $\{a, a^5, a^i p\}$ where $0 \leq i \leq 5$, which gives the products $a^2, 1, a^{i+1}p, 1, a^4, a^{i+5}p, a^{i+5}p, a^{i+1}p, a^3$. Clearly 1, $a^{i+5}p$ and $a^{i+1}p$ appear twice, so this case holds.

(v) $|x| = 3$, $|y| = 4$, $|z| = 4$ or $|x| = 6$, $|y| = 4$, $|z| = 4$

We take the subset $\{a^i, a^j p, a^k p\}$ where $i = 1, 2, 4, 5$; $0 \leq j \leq 5$, $0 \leq k \leq 5$, which gives the products $a^{2i}, a^{i+j}p, a^{i+k}p, a^{j-i}p, a^3, a^{j-k+3}, a^{k-i}p, a^{k-j+3}, a^3$. We already have the product a^3 repeated once, so we need only find one more repetition. We note that for fixed i only the difference (mod 6) between j and k matters, not the particular values (independent of i). For example $i = 1$, $j = 0$, $k = 1$ will yield the same repetition as

$i = 1$, $j = 1$, $k = 2$. So with this in mind we examine all necessary cases for values of i, j and k.

- If $i = 1$, we have the products $a^2, a^{1+j}p, a^{1+k}p, a^{j-1}p, a^{j-k+3}, a^{k-1}p, a^{k-j+3}, a^3$.

We now check the differences between j and k using these products.

$k-j$	resulting repetition
1	$a^2 = a^{j-k+3}$
2	$a^{1+j}p = a^{k-1}p$
3	$a^{j-k+3} = a^{k-j+3}$
4	$a^{1+k}p = a^{j-1}p$
5	$a^{k-j+3} = a^2$

Hence, we get the necessary repetition for all values of j and k when $i = 1$.

- If $i = 2$, we have the products $a^4, a^{2+j}p, a^{2+k}p, a^{j-2}p, a^{j-k+3}, a^{k-2}p, a^{k-j+3}, a^3$.

We now check the differences between j and k using these products.

$k-j$	resulting repetition
1	$a^4 = a^{k-j+3}$
2	$a^{2+k}p = a^{j-2}p$
3	$a^{j-k+3} = a^{k-j+3}$
4	$a^{2+j}p = a^{k-2}p$
5	$a^{j-k+3} = a^4$

Hence we get the necessary repetition for all values of j and k when $i = 2$.

- If $i = 4$, we have the products $a^2, a^{4+j}p, a^{4+k}p, a^{j-4}p, a^{j-k+3}, a^{k-4}p, a^{k-j+3}, a^3$.

We now check the differences between j and k using these products.

$k-j$	resulting repetition
1	$a^2 = a^{j-k+3}$
2	$a^{4+j}p = a^{k-4}p$
3	$a^{j-k+3} = a^{k-j+3}$
4	$a^{4+k}p = a^{j-4}p$
5	$a^{k-j+3} = a^2$

Hence we get the necessary repetition for all values of j and k when $i = 4$.

- If $i = 5$, we have the products $a^4, a^{5+j}p, a^{5+k}p, a^{j-5}p, a^{j-k+3}, a^{k-5}p, a^{k-j+3}, a^3$.

We now check the differences between j and k using these products.

$k-j$	resulting repetition
1	$a^4 = a^{k-j+3}$
2	$a^{5+k}p = a^{j-5}p$
3	$a^{j-k+3} = a^{k-j+3}$
4	$a^{5+j}p = a^{k-5}p$
5	$a^{j-k+3} = a^4$

Hence we get the necessary repetition for all values of j and k when $i = 5$.

Thus we have found a repetition for all possible values of i, j, and k, which provides the two required repetitions, so this case holds.

(vi) $|x| = 4$, $|y| = 4$, $|z| = 4$ We know all the order 4 elements in G are of the form a^ip, and $|a^ip| = 4$ for all i, so $(a^ip)^2 = a^3$ for all i. Therefore, when we take any subset containing only order 4 elements their squares will all be equal to a^3, immediately giving the required two repetitions.

We have checked all possible cases, so $G = \langle p, t | p^4 = 1, t^3 = 1, pt = t^2p \rangle$ is a $B(3,7)$ group, as required.

In order to complete the proof of Theorem 3.6, a number of lemmas will be needed. Assume that G is a nonabelian $B(3,7)$ group.

Lemma 3.1 *If $x, y \in G$ are of odd order then x and y commute.*

Proof:

We assume $yx \neq xy$ and take the subset $\{x, x^{-1}, y\}$ from which we get the products $x^2, 1, xy, x^{-2}, x^{-1}y, yx, yx^{-1}, y^2$. Using our assumptions and the cancellation law, we eliminate many of the possible equalities between products and are left to investigate the following:

(i) $x^2 = y^2 \Rightarrow x^2$ and y^2 commute. But this implies that x and y commute, since $x \in \langle x^2 \rangle$ and $y \in \langle y^2 \rangle$. So this case fails. A similar argument holds for the case when $x^{-2} = y^2$.

(ii) $xy = yx^{-1} \Rightarrow y^{-1}xy = x^{-1} \Rightarrow y^{-2}xy^2 = y^{-1}x^{-1}y \Rightarrow y^{-2}xy^2 = (y^{-1}xy)^{-1}$. So we have $y^{-2}xy^2 = (x^{-1})^{-1} \Rightarrow xy^2 = y^2x$. But $y \in \langle y^2 \rangle$, therefore x and y^2 cannot commute. So this case also fails. A similar argument holds for $x^{-1}y = yx$.

All cases fail, so there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. So x and y commute. □

Lemma 3.2 *If $x \in G$ is of odd order and $y \in G$ is of order 2^m for some integer m, then x and y^2 commute.*

Proof:

We assume $y^2x \neq xy^2$ and take the subset $\{x, x^{-1}, y\}$. Multiplying in the usual way we get the products $x^2, 1, xy, x^{-2}, x^{-1}y, yx, yx^{-1}, y^2$. Using our assumptions and the cancellation law, we eliminate many of the possible equalities between products and are left to investigate the following:

(*i*) $x^2 = y^2 \Rightarrow x^2$ and y^2 commute. Since x has odd order we know that $x \in \langle x^2 \rangle$. But this means then that x and y^2 commute, so this case fails. A similar argument follows for the case where $x^{-2} = y^2$.

(*ii*) $x^{-1}y = yx^{-1} \Rightarrow y = xyx^{-1} \Rightarrow yx = xy$, which is clearly a contradiction, so this case fails.

(*iii*) $xy = yx^{-1} \Rightarrow y^{-1}xy = x^{-1} \Rightarrow y^{-2}xy^2 = y^{-1}x^{-1}y \Rightarrow y^{-2}xy^2 = (y^{-1}xy)^{-1}$, and since $x^{-1} = y^{-1}xy$, we get $y^{-2}xy^2 = (x^{-1})^{-1} \Rightarrow xy^2 = y^2x$, clearly a contradiction. A similar argument follows for the case where $x^{-1}y = yx$.

All cases fail, so there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. Consequently, x and y^2 commute. □

Lemma 3.3 *If $x \in G$ is of odd order greater than 3 and $y \in G$ is of order 2^m for some integer m, then x and y commute.*

Proof:

Again, we assume $yx \neq xy$ and take the subset $\{x, x^2, y\}$. Multiplying in the usual way we get the products $x^2, x^3, xy, x^4, x^2y, yx, yx^2, y^2$. Using our assumptions and the cancellation law, as before, we eliminate many of the possible equalities between products and are left to investigate the following:

(*i*) $x^2 = y^2 \Rightarrow |x^2|$ is even, which we know is false since $|x|$ is odd. A similar argument holds for the cases where $x^3 = y^2$, $x^4 = y^2$ (for $x^3 = y^2$, note that $|x| > 3$).

(*ii*) $xy = yx^2 \Rightarrow y^{-1}xy = x^2 \Rightarrow y^{-1}xy = (yx^2y^{-1})^2$ since $x = yx^2y^{-1}$. But then $y^{-1}xy = yx^2y^{-1}yx^2y^{-1} = yx^4y^{-1} \Rightarrow x = y^2x^4y^{-2}$. Applying the last lemma, it is

clear that x and y^2 commute giving $y^2x^4y^{-2} = x^4y^2y^{-2} = x^4 \Rightarrow x^4 = x \Rightarrow x^3 = 1$. This contradicts our assumption that $|x|$ is greater than 3, so this case fails. The case where $x^2y = yx$ fails by a similar argument.

(iii) $yx^2 = x^2y \Rightarrow x^2$ and y commute. Since $|x|$ is odd, $x \in \langle x^2 \rangle$ which contradicts the fact that $xy \neq yx$, hence this case fails.

Since all cases fail, there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. Therefore, x and y commute. □

Lemma 3.4 *If $x, y \in G$ are both of order 3 with $y \neq x$ and $y \neq x^2$, and $z \in G$ is of order 2^m for some integer m, then z commutes with both x and y.*

Proof:

We may assume that z does not commute with either x or y (replacing x or y with xy if needed. Since x and y commute by Lemma 3.1, $(xy)^3 = x^3y^3 = 1$, $y \neq x^2 \Rightarrow xy \neq 1$, so $|xy| = 3$ and $xy \neq x$, $xy \neq x^2$). It is clear also that z doesn't commute with x^2 or y^2. Thus if $z^{-1}xz = y$ we replace y with y^2, so we can assume $z^{-1}xz \neq y$. Also, it follows from Lemma 3.2 that $z^{-1}yz \neq z^{-2}xz^2 = x$, so we consider the subset $\{x, y, z\}$ and multiply in the usual way to get the products $x^2, xy, xz, y^2, yz, zx, zy, z^2$. Using the above assumptions and the cancellation law, we are left to investigate the following.

(i) $x^2 = y^2 \Rightarrow x^4 = y^4 \Rightarrow x = y$, clearly a contradiction since we assume $x \neq y$, so this case fails.

(*ii*) $x^2 = z^2 \Rightarrow |x^2| = |z^2|$ which is clearly a contradiction since $|x^2| = 3$ and $|z^2|$ is a power of 2. A similar argument holds for the cases $y^2 = z^2$ and $xy = z^2$.

(*iii*) $x^2 = yz \Rightarrow y^2x^2 = z$ which is a contradiction since $|y^2x^2| = 3$ and $|z|$ is a power of 2. A similar argument holds for $x^2 = zy$, $y^2 = xz$ and $y^2 = zx$.

All cases fail, so there are no two products from our list that are equal, contradicting the fact that G is $B(3,7)$. Therefore, z commutes with both x and y. □

Lemma 3.5 *If $x \in G$ is of order 3, $y \in G$ is of odd order greater than 3, and $z \in G$ is of order 2^m for some integer m, then z commutes with both x and y.*

Proof:

We know from Lemma 3.3 and Lemma 3.1 above that y commutes with z, and x commutes with y. If we say $|y| = n$, then $(xy)^{3n} = x^{3n}y^{3n} = 1 \cdot 1 = 1$, so the order of xy divides $3n$. Since $3n$ is odd, $|xy|$ is also odd. (Note that $y \neq x^2$ so $xy \neq 1$, and $(xy)^3 = 1 \Rightarrow x^3y^3 = 1 \Rightarrow y^3 = 1$ which is a contradiction since $|y|$ is of order greater than 3. So $|xy|$ is odd and greater than 3). Since $|xy| = lcm(3,n)$, $|xy|$ is odd and greater than 3, thus Lemma 3.3 says that xy commutes with z, and therefore x also commutes with z. □

We will now use the previous lemmas to obtain information on the structure of G when G is a $B(3,7)$ group. In what follows, T will be the set $T = \{g \in G \mid$ the order of g is odd$\}$.

Lemma 3.6 *The set T is an abelian normal subgroup of G.*

Proof:

For all $t \in T$, it follows from Lemma 3.1 that $t_1 t_2^{-1} = t_2^{-1} t_1$. So $|t_1 t_2^{-1}| = lcm(|t_1|, |t_2|)$ is odd, and thus $t_1 t_2^{-1} \in T$. This shows that T is an abelian subgroup. Also, $|gtg^{-1}| = |t|$ for $t \in T$ and $g \in G$, so $gtg^{-1} \in T$, and therefore $T \triangleleft G$. □

Lemma 3.7 *Let P be a Sylow 2-subgroup of G. Then $G = TP$.*

Proof:

Since $T \triangleleft G$, it follows that $TP = \{tp | t \in T, p \in P\}$. Hence $|TP| = \frac{|T||P|}{|T \cap P|} = |T||P|$ since $|T \cap P| = 1$. So $G = TP$, as required. □

Lemma 3.8 *There are two possibilities for T, either $|T| = 3$ or T is central in G.*

Proof:

Assume that $|T| > 3$ and let $x \neq 1$ be any element of T. Let $z \in G$ be such that $|z| = 2^n$ for some n. If $|x| > 3$, then Lemma 3.3 says that x and z commute. On the other hand, if $|x| = 3$ we can choose $y \in T$ such that $y \notin \langle x \rangle$ (since $|T| > 3$). It follows from Lemmas 3.4 and 3.5 that z commutes with both x and y.

So in all cases x and z commute and we conclude from Lemma 3.7 that x is central. Thus T is central. □

Lemma 3.9 *If T is central in G then $T = \{1\}$.*

Proof:

If P is a Sylow 2-subgroup of G, then P is nilpotent and nonabelian because $G = T \times P$ and T is central in G with G nonabelian. So there exists $k \geq 1$ such that $Z_k(P) \neq P$ while $Z_{k+1}(P) = P$. We know that $\frac{Z_k(P)}{Z_{k-1}(P)}$ is the centre of $\frac{P}{Z_{k-1}(P)}$ and $\frac{P}{Z_k(P)}$ is abelian but not cyclic, which allows us to choose maximal subgroups $M \neq N$ of P such that $M \supseteq Z_k(P)$ and $N \supseteq Z_k(P)$. So we have $|\frac{P}{M}| = |\frac{P}{N}| = 2$ and $|\frac{P}{M \cap N}| = 4$.

Next, we want to choose $a \in M - N$ and $b \in N - M$ such that $ab \neq ba$. Assume instead we have chosen $a \in M - N$ and $b \in N - M$ such that $ab = ba$ (note that $P = \langle M \cap N, a, b \rangle$). Since a is not in N and $N \supseteq Z_k(P) \supseteq Z(P)$, a is not in $Z(P)$. But, from our assumption, a commutes with both a and b, so there must exist an $x \in M \cap N$ with $xa \neq ax$. Then $bx \in N - M$ and $abx \neq bxa$. So if we pick a and b such that $ab = ba$, we simply replace b by bx.

Next, let $t \in T$, $t \neq 1$. If we select $S = \{a, bt, abt^2\}$, where a and b are chosen as before, then S^2 contains the nine elements $a^2, abt, a^2bt^2, bat, b^2t^2, babt^3, abat^2, ab^2t^3, ababt^4$. We now try to show that more than seven of these are distinct. If $t^3 \neq 1$ this is straightforward, so we will assume that $t^3 = 1$ from now on. We use the cancellation law with the fact that $ab \neq ba$ to eliminate most of the possibilities and we are left to investigate the following:

• If we take $bab = a^2 \Rightarrow b^{-1}ab = b^{-2}a^2 \in M \cap N \Rightarrow a = b(b^{-2}a^2)b^{-1} \in M \cap N$. But then this implies that $a \in N$, a contradiction, so bab and a^2 are distinct. A similar argument holds for the case where $b^2t^2 = abat^2$.

• If we let $ababt = bat$ then $a^{-1}ba = bab = b^2(b^{-1}ab) \in M$, which contradicts $b \in N - M$. So these products are distinct.

We are left with more than seven distinct products, hence no such t can be chosen to satisfy the condition that G is $B(3,7)$. Thus $T = \{1\}$ as required. □

Now we will proceed with the proof of Theorem 3.6. We may assume that G is not a 2-group and $|G| = 3 \cdot 2^n$ for some n, that G has a unique Sylow 3-subgroup $T = \langle t \rangle$ where $t^3 = 1$, and that T is not central in G. Let P be a Sylow 2-subgroup of G, so $G = TP$.

Next, we set $Q = \{x \in P | xt = tx\}$. Since T is not central in G, $P \neq Q$. Note that if $\alpha \in P - Q$, then $\alpha t \alpha^{-1} = t^2$ and $\alpha t^2 \alpha^{-1} = (\alpha t \alpha^{-1})^2 = (t^2)^2 = t^4 = t$. It follows that if $\alpha_1 \in P - Q$ and $\alpha_2 \in P - Q$ then $\alpha_1\alpha_2 \in Q$, since $\alpha_1\alpha_2 t(\alpha_1\alpha_2)^{-1} = \alpha_1\alpha_2 t\alpha_2^{-1}\alpha_1^{-1} = \alpha_1 t^2 \alpha_1^{-1} = t$. So Q is of index 2 in P. Note that since $|G| \geq 8$, $|P| > 2$ it follows that $|Q| \geq 2$. We must now check two cases:

Case 1: P is abelian

We choose (if possible) $p \in P - Q$ and $q \neq 1 \in Q$ with $p^2 \neq q$, and let $S = \{pq, tp, tq\}$. Multiplying the elements of S in the usual way, we get the products $p^2q^2, pqtp, pq^2t, tp^2q, tptp, tptq, tpq^2, t^2qp, t^2q^2$. Using the earlier remark that $\alpha t \alpha^{-1} =$

t^2, this list can be rewritten as $p^2q^2, p^2qt^2, pq^2t, p^2qt, p^2, pq, pq^2t^2, pqt, q^2t^2$. The cancellation law tells us that the only possibility for equality here is $p^2q^2 = p^2$. So there must be at least eight distinct products, giving a contradiction. It follows then that we must have $p^2 = q$.

We can conclude that $P = \langle p \rangle$ must be cyclic of order 4. Therefore the group in question is exactly $G = \langle p, t | p^4 = 1, t^3 = 1, pt = t^2p \rangle$ of order 12.

Case 2: P is not abelian

First we need a lemma from [2]. This result could be deduced from the argument given in the second paragraph of the proof of Lemma 3.9, but we will include it for completeness.

Lemma 3.10 *Let P and Q be as defined above. Either P is abelian or there are elements $a \in P - Q$ and $b \in Q$ such that $ab \neq ba$.*

Proof:

If $a \in P - Q$ centralises Q, then a centralises $\langle a, Q \rangle = P$, that is, $a \in Z(P)$. Thus if each element of $P - Q$ centralised Q, then each element of $\langle P - Q \rangle$ would centralise Q and hence would lie in $Z(P)$. We know that $P - Q \subseteq Z(P)$ contains exactly half of the elements of the subgroup P since Q is of index 2, but also $1 \in Q$ and $1 \in Z(P)$. Therefore $\langle P - Q \rangle = P$ and $P = Z(P)$. So P is abelian. □

We return to the proof of Theorem 3.6, assuming P is not abelian and choosing a and b as in Lemma 3.10.

We choose two particular subsets.

(i) First, we choose the subset $S = \{a, b, t\}$, with $a \in P - Q$, $b \in Q$, $t \in T$ as before. Multiplying in the usual way we get the products $a^2, ab, at, ba, b^2, bt, ta, tb, t^2$. Since $bt = tb$ by definition, we use our assumptions above and the cancellation law to eliminate all other possible equalities except for $a^2 = b^2$. So we get eight distinct products unless $a^2 = b^2$. Note that we can replace $a \in S$ by $ab \in P - Q$ since $(ab)b \neq b(ab)$, which gives us $abab = b^2$.

(ii) We now choose another subset $S = \{a, tb, t\}$. Multiplying the elements of S we get the eight products $a^2, atb, at, tba, t^2b^2, t^2b, ta, t^2$, which can be rewritten as $a^2, abt, at, bat^2, b^2t^2, bt^2, at^2, t^2$. Clearly, the only possible equality is $b^2t^2 = t^2$, forcing $b^2 = 1$. So we get eight distinct products unless $b^2 = 1$.

If we combine these subcases, we get $a^2 = b^2 = abab = 1$ which implies that $aba = b \Rightarrow aba^2 = ba \Rightarrow ab = ba$, contradicting our assumption that $ab \neq ba$. Since Case 2 cannot possibly exist, the proof of Theorem 3.6 is complete. □

For $B(3, 8)$ groups, the classification of the 2-group case (case (ii) from Theorem 3.5) had been partly solved by Berkovich, Freiman, and Praeger [2]. Before stating this theorem, we must define two families of groups.

Definition 3.1 *A 2-group G is called a D-group if it is nonabelian and the subgroup $A = \langle x | x \in G, x^2 \neq 1 \rangle$ is a proper subgroup of G.*

Definition 3.2 *A 2-group G is called a Q-group if it is nonabelian and satisfies the following conditions:*

(i) G has a subgroup A of index 2 such that each element of $G - A$ has order 4, and

(ii) If $x, y \in G - A$ then $x^2 = y^2$ and $a^x = x^{-1}ax = a^{-1}$ for all $a \in A$.

Now that we have defined D-groups and Q-groups, the theorem is as follows.

Theorem 3.7 *Let G be a nonabelian $B(3,8)$ 2-group. Then either*

(i) G is a D-group or a Q-group, or

(ii) G has exponent 4 and derived length 2. Further, each of the centre $Z(G)$ and the derived quotient G/G' is either elementary abelian or the product of an elementary abelian group and a cyclic group of order 4.

Conversely, each 2-group which is a D-group or a Q-group is also a $B(3,8)$ group.

Later, case (ii) from Theorem 3.7 was completed by Longobardi and Maj [7]. Their theorem is as follows.

Theorem 3.8 *Let G be a finite 2-group of exponent 4. Then G is $B(3,8)$ if and only if one of the following holds:*

(i) G is abelian,

(ii) $\Omega_1(G) = \langle x^2 | x \in G \rangle$ has order 2,

(iii) $G = \langle A, x \rangle$, where A is abelian, $x^2 \in A$, $a^x = a^{-1}$ for every $a \in A$,

(iv) $G = E_2 \times \langle a, b, c \rangle$, $|a| = |b| = |c| = 4$, $a^b = a^{-1}$, $[a, c] = [b, c] = 1$, $c^2 = a^2b^2$,

(v) $G = E_2 \times \langle a, b, c, d \rangle$, $a^b = a^{-1}$, $c^b = c^{-1}$, $c^d = c^{-1}$, $[a, c] = [a, d] = [b, d] = 1$, $|a| = |b| = |c| = |d| = 4$, $c^2 = d^2 = a^2b^2$.

We do not have a proof classifying which 2-groups are $B(3, 7)$. However, we are able to show that a nonabelian 2-group of order ≤ 16 is $B(3, 7)$ if and only if it is a Hamiltonian 2-group. Here, we present some groups that we know are not $B(3, 7)$.

- $\underline{D_8}$

If we take the subset $S = \{a, b, ab\}$, we get the products $a^2, ab, a^2b, a^3b, 1, a^3, b, a, 1$, of which the only repetition is the identity. We get eight distinct products, so D_8 is not $B(3, 7)$.

- $\underline{D_{2^n}}$

All the dihedral groups of order 2^n for some $n \geq 3$ contain a subgroup $H \cong D_8$, so the subset $S = \{a, b, ab\}$ previously chosen will yield eight distinct products in each case. Therefore none of this family of dihedral groups can be $B(3, 7)$.

- $\underline{D_{16}^+ = \langle a, b | a^8 = b^2 = 1, ba = a^5b \rangle}$

If we take the subset $S = \{a, b, ab\}$, we get the products $a^2, ab, a^2b, a^5b, 1, a^5, a^6b, a, a^6$. We get nine distinct products, so therefore D_{16}^+ is not $B(3, 7)$.

- $\underline{D_{16}^- = \langle a, b | a^8 = b^2 = 1, ba = a^3b \rangle}$

If we take the subset $S = \{a, b, ab\}$, we get the products $a^2, ab, a^2b, a^3b, 1, a^3, a^4b, a, a^4$. We get nine distinct products, so therefore D_{16}^- is not $B(3, 7)$.

- $\underline{P = \langle a, b | a^4 = b^4 = 1, ba = a^3 b \rangle}$

If we take the subset $S = \{a, b, ab\}$, we get the products $a^2, ab, a^2b, a^3b, b^2, a^3b^2, b, ab^2, b^2$, of which the only repetition is b^2. In this case, we get eight distinct products, so therefore P is not $B(3,7)$.

- $\underline{Q_{16} = \langle a, b | a^8 = 1, a^4 = b^2, ba = a^7 b \rangle}$

If we take the subset $S = \{a, b, ab\}$, we get the products $a^2, ab, a^2b, a^7b, a^4, a^3, b, a^5, a^4$, of which the only repetition is a^4. Again, we get eight distinct products, so therefore Q_{16} is not $B(3,7)$.

- $\underline{H = \langle a, b | a^4 = b^4 = (ab)^2 = (a^2, b) = 1 \rangle}$

If we take the subset $S = \{a, b, ab\}$, we get the products $a^2, ab, a^2b, a^3b^3, b^2, a^3, b^3, ab^2, 1$, of which we find no repetitions. Here, we get nine distinct products, so therefore H is not $B(3,7)$.

- $\underline{D = \langle a, b, c | a^2 = b^2 = c^4 = 1, ac = ca, bc = cb, ba = c^2 ab \rangle}$

If we take the subset $S = \{ca, cb, cab\}$, we get the products $c^2, c^2ab, c^2b, ab, c^2, a, b, c^2a, 1$, of which c^2 is the only repetition. We get eight distinct products, so D is not $B(3,7)$.

Since $D_8 \times C_2$ contains D_8 as a subgroup, we have eliminated all nonabelian groups of orders 8 and 16, except for the Hamiltonian 2-groups. This fact gives rise to the following theorem.

Theorem 3.9 *$G = Q_8 \times C_2 \times \cdots \times C_2$ is a $B(3,7)$ group.*

Proof:

We begin by looking at Q_8 by itself. We know that Q_8 has one element of order 2, namely a^2, and every other element (besides the identity) is of order 4, which implies that the square of every order 4 element in Q_8 will be a^2. Since 1 and a^2 are central, any 3-subset involving these must have at least two repeated products. It follows that the only case to consider is $S = \{x, y, z\}$ where $|x| = |y| = |z| = 4$. But then $x^2 = y^2 = z^2 = a^2$ yielding two repetitions. Thus Q_8 is a $B(3,7)$ group.

However, it is easy to see that the same argument as above also applies to $Q_8 \times C_2 \times \ldots C_2$. In that group, all elements of order ≤ 2 are central and all non-central elements square to $(a^2, 1, \ldots, 1)$. So, as above, we conclude that $Q_8 \times C_2 \times \ldots C_2$ is $B(3,7)$. $\square$

As mentioned above, the situation for $B(3,7)$ groups is still open. Using the above results, we would like to suggest the possibility that the group of order 12, which appeared in Theorem 3.6, and the Hamiltonian 2-groups are the only nontrivial, nonabelian $B(3,7)$ groups.

Chapter 4

$B(4,k)$ and $B(5,k)$ groups

We begin a survey of higher n values with $B(4,k)$ groups. As usual our first concern is the case $k = \frac{n(n+1)}{2} = \frac{4(5)}{2} = 10$. We have the following theorem from Parmenter [8].

Theorem 4.1 *There are no nontrivial, nonabelian $B(4,10)$ groups.*

Before we get into proving Theorem 4.1, we first need to prove the following lemma.

Lemma 4.1 *If x, y are noncommuting elements of a $B(4,10)$ group, then $\langle x, y\rangle$ is isomorphic to one of S_3, D_8, Q_8, D_{10}.*

Proof: As in some of our earlier proofs, we must examine a number of cases. The procedure will be to let x and y be noncommuting elements of a nonabelian $B(4,10)$ group, and look at different combinations for the orders of x and y. Here we will only mention repetitions between products that are not immediately obtainable by the cancellation law.

• Assume that $x^2 = 1$ and y is of order 8. If we take the subset $\{x, y, y^2, y^3\}$, we get at least nine distinct products 1, xy, xy^2, xy^3, y^2, y^3, y^4, y^5, y^6. Hence, one of yx and y^3x must be equal to one of these nine elements. Since $yx = xy^2$ implies that $y = xy^2x = xyxy^2 = x^2y^4 = y^4$ which is impossible, the only possibility for yx is $yx = xy^3$. Also $y^3x = xy^3$ implies $yx = xy$ since $y^3 \in \langle y \rangle$, so the only possibility for y^3x is $y^3x = xy$. So yx must equal xy^3 in either case. But then if we take the subset $\{x, y, xy, y^2\}$, we get eleven distinct products, namely 1, xy, y, xy^2, yx, y^2, yxy, y^3, $xyxy$, y^2x, y^2xy. This is a contradiction, so this case does not occur.

• Assume that $x^2 = 1$ and that the order of y is greater than 6 but not equal to 8. We take the subset $\{x, y, y^2, y^3\}$ as before, and this time we get the ten distinct elements 1, xy, xy^2, xy^3, yx, y^2, y^3, y^4, y^5, y^6, noting that $yx = xy^2$ implies that $y = y^4$ as before and, similarly, $yx = xy^3$ implies $y = y^9$, which are impossible. It now follows that y^2x must equal one of these ten elements and the only possibilities are $y^2x = xy^2$ or $y^2x = xy^3$, noting that $y^2x = xy$ implies that $y = x^2y = y^4$, as before. Similarly, we must have $y^3x = xy^2$ or $y^3x = xy^3$. But to have $y^2x = xy^2$ and $y^3x = xy^3$ together implies $yx = xy$, while $y^2x = xy^3$ and $y^3x = xy^2$ together give $y^6x = y^4(y^2x) = y^4xy^3 = y^2xy^6 = xy^9$ and $y^6x = y^3(y^3x) = y^3xy^2 = xy^4$, which imply that $xy^9 = xy^4 \Rightarrow y^5 = 1$. All possibilities yield a contradiction, so this case cannot occur.

• Assume that $x^2 = 1$ and y is of order 6. Taking the same subset $\{x, y, y^2, y^3\}$, we get the nine distinct elements 1, xy, xy^2, xy^3, yx, y^2, y^3, y^4, y^5. So either y^2x or y^3x

must equal one of these nine elements, thus we can eliminate all possibilities similarly to the last case except for $y^2x = xy^2$ or $y^3x = xy^3$. If we set $y^2x = xy^2$ and take the subset $\{x, y, xy, y^3\}$, we get the eleven distinct products 1, xy, y, xy^3, yx, y^2, yxy, y^4, xy^2, y^3x, y^3xy. Also, if $y^3x = xy^3$, we obtain from the subset $\{x, y, xy, y^2\}$ the eleven distinct products 1, xy, y, xy^2, yx, y^2, yxy, y^3, xy^3, y^2x, y^4. Since all possibilities fail, we again have a contradiction.

• Next we assume $x^2 = 1$ and $y^5 = 1$. This time we take the subset $\{x, y, xy, y^2\}$ and get the ten distinct products 1, xy, y, xy^2, yx, y^2, yxy, y^3, xy^3, y^4. Note that $yx = xy^2$ implies $y = y^4$ and $xy^3 = yx$ implies $y = y^9$, as before. Now y^2x must equal one of these ten elements and the only possibility is $y^2x = xy^3$, since $y^2x = xy$ implies $y = y^4$ and $y^2x = xy^2$ implies $yx = xy$. But, if this is the case, then $yx = y^6x = y^4(y^2x) = y^4xy^3 = y^2xy^6 = y^2xy = xy^4$. So in this case we have $\langle x, y\rangle \cong D_{10}$, which was one of our four possible groups.

• Next, we take $x^2 = 1$ and y of order 4. If $yx = xy^3$, then $\langle x, y\rangle \cong D_8$, so we assume this is not the case. But then if we take the subset $\{x, y, xy, y^3\}$, in a similar way as before, we get the eleven distinct products 1, xy, y, xy^3, yx, y^2, yxy, xy^2, x, y^3x, y^3xy, which yields a contradiction.

• Here we assume that $x^2 = 1 = y^3$. If $yx = xy^2$ then $\langle x, y\rangle \cong S_3$, so we assume this is not the case. Again, taking the subset $\{x, y, xy, y^2\}$, we get the ten distinct products 1, xy, y, xy^2, yx, y^2, yxy, x, y^2x, y^2xy. So xyx must equal some element from this list. The only possibilities are $xyx = yxy$ or $xyx = y^2xy$, but $xyx = yxy$ implies

$xy = xyx^2 = yxyx = y^2xy \Rightarrow y^2 = 1$ and $xyx = y^2xy$ implies that $yx = x^2yx = xy^2xy = xyx^2yxy = y^2(xyx)yxy = y^2y^2xyyxy = yxy^2xy = yxxyx = y^2x \Rightarrow y = 1$. So both cases fail, giving a contradiction. We note here that the argument provided for this case is shorter than that in [8].

• If $x^2 = 1 = y^2$ then $(xy)^2 \neq 1$ (since $xy \neq yx$), so replacing y by xy we can assume we are dealing with one of the cases already considered.

In order to finish the argument, we need to check the cases where neither x nor y is of order 2.

• We first assume that $x^2 \neq 1$, $y^2 \neq 1$ and $x^2 = y^2$. If $yx = xy^3$, it will then follow that $y^3 = yx^2 = xy^3x = y^7$, so $y^4 = 1$ and $G \cong Q_8$. Hence, we may assume that $yx \neq xy^3$. If we take the subset $\{x, x^3, y, xy\}$, then we get the ten distinct elements x^2, x^4, xy, x^2y, x^3y, x^4y, yx, yx^3, yxy, xy^2 (note that $x^3 \neq 1$ since $x^2 = y^2$, and also $yx^3 = xy$ implies $xyx = yx^4 = y(y^2)(y^2) = x^4y$). Hence xyx must be equal to some element from this list and, by the cancellation law, the only possibility is $xyx = yxy$. But this would make xyx^3 distinct from all elements in the list, so we have a contradiction.

• Next we assume that $x^2 \neq 1$, $y^2 \neq 1$, $x^2 \neq y^2$, $xyx \neq y$ and $yxy \neq x$. We may also assume $(xy)^2 \neq 1$ because otherwise we would be in one of the previous cases. If we take the subset $\{1, x, y, xy\}$, we get the twelve elements 1, x, y, xy, x^2, x^2y, yx, y^2, yxy,xyx, xy^2, $xyxy$. We need two of these products to be equal to other elements in the list or we will have a contradiction. However, by the cancellation law

and the given conditions, the only possibilities are $yx = x^2y$, $yxy = x^2$, $xyx = yxy$, $xyx = y^2$, $xy^2 = yx$, $xyxy = yx$. The condition $yx = x^2y$ contradicts each of the other five possible conditions, so we can assume this condition doesn't hold, and the same remark is true for $yx = xy^2$ and $xyxy = yx$. Next, we observe that $yxy = x^2$ and $xyx = yxy$ cannot be true at the same time since together they imply that $y = 1$. A similar argument shows that $xyx = yxy$ and $xyx = y^2$ also cannot be true at the same time. So the only remaining possibility is $yxy = x^2$ and $xyx = y^2$. However, under these assumptions, if we take the subset $\{x, y, xy, x^2\}$ we get the eleven distinct products x^2, xy, x^2y, x^3, yx, y^2, yx^2, xy^2, xyx^2, x^3y, x^4. We cannot get two of the six conditions to hold simultaneously, so this case fails.

The last three cases all assume that $x^2 \neq 1$, $y^2 \neq 1$, $x^2 \neq y^2$, and $xyx = y$. Once these possibilities have been settled, we will be finished because a similar (symmetrical) argument will be true when $yxy = x$. Note that $yx = x^{-1}y$ means that $y^nx = x^{-1}y^n$ whenever n is odd, and therefore this forces the order of y to be even.

• First, we make the above assumptions and also assume that the order of y is greater than 4 but not equal to 8. Then, if we take the subset $\{1, x, y, y^3\}$, we get the eleven distinct elements 1, x, y, y^3, x^2, xy, xy^3, yx, y^2, y^4, y^3x. We note that $x^2 = y^3$ implies $xy^3 = y^3x = x^{-1}y^3 \Rightarrow x = x^{-1} \Rightarrow x^2 = 1$, and either of $yx = xy^3$ or $xy = y^3x$ implies that $x^2 = y^2$, since $yx = xy^3 \Rightarrow yx^2 = xy^3x = xx^{-1}y^3 = y^3 \Rightarrow x^2 = y^2$ and $xy = y^3x = x^{-1}y^3 \Rightarrow x^2 = y^2$. Finally if $y^4 = x^2$, then $y^5 = yx^2 = x^{-2}y = y^{-3}$ $\Rightarrow y^8 = 1$, so this case fails.

• Next we consider the case where the order of y is 8. If we take the subset $\{1, x, y, y^3\}$, we get the ten distinct elements 1, x, y, y^3, x^2, xy, xy^3, yx, y^2, y^3x. So y^4 must be equal to an element from this list and the only possibility is $y^4 = x^2$. But, if this is the case, then $(y^3)^2 = y^6 = x^2y^2 = y^2x^2$ is distinct from all ten elements, so we have a contradiction.

• Finally, we assume that y is of order 4. If we take the subset $\{x, y, xy, y^2\}$ we get the nine distinct products x^2, xy, x^2y, xy^2, y^2, y^3, xyx, xy^3, 1. It follows then that either yx or yxy must be equal to one of the listed elements, the only possibilities being $yx = x^2y$ or $yxy = x^2$. If $yx = x^2y$, then $xyx = x^3y \Rightarrow y = x^3y \Rightarrow x^3 = 1$ (since $xyx = y$ from above), but then the subset $\{xy^2, y, x^2, x^2y\}$ gives the eleven distinct elements $xy^2xy^2 = xyx^2yy^2 = xx^2yxy^3 = x^2y^4 = x^2$, xy^3, $xy^2x^2 = xyx^2yx = xyx^2x^2y = xyxy = xx^2yy = y^2$, $xy^2x^2y = y^3$, $yxy^2 = x^2y^3$, $yx^2 = xy$, $yx^2y = xy^2$, x^2y, x, x^2y^2, $x^2yx^2 = y$. On the other hand, if we let $yxy = x^2$, then $y^2 = x^3$ and then the subset $\{x, y, x^2, x^2y\}$ will give us the eleven distinct elements x^2, xy, x^3, x^3y, yx, yx^2, yx^2y, x^2y, x^4, x^2y^2, x^2yx^2. So, under both conditions, we get a contradiction, and the proof is complete. □

We can now use the above lemma to prove Theorem 4.1.

Proof: (Theorem 4.1) Let x, y be noncommuting elements from a nonabelian $B(4, 10)$ group G. Then $\langle x, y\rangle$ is isomorphic to one of S_3, D_8, Q_8 or D_{10}, from Lemma 4.1. So we need to prove that $G = \langle x, y\rangle$ in all cases.

• First, we assume that $\langle x, y\rangle \cong D_8$ or D_{10}, whence we may also assume that $x^2 = 1$, $y^4 = 1$ or $y^5 = 1$, and $yx = xy^{-1}$. Note that if we take the subset $\{x, y, xy\}$, we get the eight distinct elements 1, xy, y, yx, y^2, yxy, xyx, xy^2. It follows that, if we take some $z \notin \langle x, y\rangle$, we would get eleven distinct elements from the subset $\{x, y, xy, z\}$, which is a contradiction. So $\langle x, y\rangle \cong G$, as required.

• Next assume $\langle x, y\rangle \cong Q_8$ and $x^4 = 1$, $y^2 = x^2$, $yx = xy^3$ with $z \notin \langle x, y\rangle$. We can assume that z does not commute with x (if it does, we use yz). By Lemma 4.1, since $\langle x, z\rangle$ contains an element of order 4, we know that $\langle x, z\rangle \cong D_8$ or $\langle x, z\rangle \cong Q_8$. But, if $\langle x, z\rangle \cong D_8$, then $\langle x, z\rangle = G$ by the previous case. So we assume that $\langle x, z\rangle \cong Q_8$. It then follows readily that $z^2 = x^2 = y^2$ and $zx = xz^3$. If we take the subset $\{x, y, xy\}$, we get the seven distinct elements x^2, xy, x^2y, yx, yxy, xyx, xy^2. Furthermore, the elements xz, yz, xyz, zx are distinct, so the subset $\{x, y, xy, z\}$ will give us eleven distinct products, and therefore a contradiction. So again $G = \langle x, y\rangle$.

• Finally we assume that $\langle x, y\rangle \cong S_3$ and $x^2 = 1$, $y^3 = 1$, $yx = xy^2$. Again, if $z \notin \langle x, y\rangle$, we may then assume that z does not commute with x, and the only case not settled is where $\langle x, z\rangle \cong S_3$. We may assume z is of order 3 (or use xz if necessary), and so $zx = xz^2$. But now the subset $\{x, y, xy, z\}$ contains all six elements of $\langle x, y\rangle$ in addition to xz, yz, xyz, z^2, and zx. Since we now have eleven elements in total and therefore a contradiction, $G = \langle x, y\rangle$.

We have shown that $G = \langle x, y\rangle$ in all cases, so the proof is complete. □

We see that the theorem for $B(4,10)$ groups is similar to that for $B(3,6)$ groups. This might lead us to believe that the same statements will appear for higher values of n. However, this trend stops at $n = 5$ due to the following theorem.

Theorem 4.2 *The group $G = Q_8 \times C_2$ is a $B(5,15)$ group.*

Proof: We first note that the center $Z(G)$ is an elementary abelian 2-group of order 4, and that one particular element of $Z(G)$, say h such that $h = (a^2, 1)$, has the property that $x^2 = h$ for all noncentral elements x of G. In addition, if a product xy of noncentral elements x, y is noncentral in G then $yx = xyh$.

We assume that G is not a $B(5,15)$ group and take a subset $\{v, w, x, y, z\}$ of G such that every element of G is a product of two elements from the subset. We observe that each of v^2, w^2, x^2, y^2, z^2 must equal 1 or h. So we immediately have at least three repeated products from these squares alone. We now look at three cases, namely when we have 0, 1, or 2 central elements in the subset. We note that a choice of three or more central elements produces more than enough equal products simply by commutativity.

- If we have v and w central, then v and w would give seven more repeated products. In this case, we have at least ten repetitions out of twenty-five products which contradicts the assumption.

- If we have v central and $w^2 = x^2 = y^2 = z^2 = h$, then we have seven repeated products, namely x^2, y^2, z^2, wv, xv, yv, and zv. Since each element of G is a product of two elements from the subset and there are four central elements, some product

of different noncentral elements must be in $Z(G)$ and not equal to 1 or h. If we assume wx is this product (by relabelling if necessary), then $wx = xw$ giving an eighth repeated product. Also, for the same reason there has to exist another product that must equal the fourth element of $Z(G)$, giving a ninth repeated product. If this product involves w or x, we can construct another central product (i.e. if wy is central, then so is $xy = (xw)w^2(wy)$), which would be a tenth repeated product and therefore a contradiction. So the only possibility is that $yz \in Z(G)$. But now $(xz)(yw) = x(zy)w = (xw)(zy) = h$, since it is the product of the two distinct elements of $Z(G)$ which are different from 1 and h. But, for this to happen in G, either xz and yw are central or $xz = yw$. In either case, we have a tenth repeated product which is a contradiction.

- If we have $v^2 = w^2 = x^2 = y^2 = z^2 = h$, then we have no central elements in our subset and we immediately have four repeated products. So, in this situation, we must be able to obtain the three central elements other than h as products of two elements from the subset. We know that some element in $\{v, w, x, y, z\}$ must be used twice in these products and by relabelling, if necessary, we can assume vw and vx are central. But then $wx = wv(v^2)vx$ is also central, as we saw in the last case, thus we now have seven repeated products. Since vw, vx, and wx are all different and none of them is equal to h, we may assume that $vw = 1$ and it then follows that $w = vh$. Next, we observe that if vy or vz were central, then we would be able to find three additional central elements, similarly to the last case, by getting more repeated

products and, hence, a contradiction. So we can assume that none of the products is central. But then $vy = yvh = yw$, $yv = vyh = wy$, $vz = zvh = zw$, giving us three additional repeated products, which is a contradiction.

The three possible cases all contradict the assumption that G is not $B(5, 15)$, so the proof is complete. □

In fact, G has the interesting property that it is the only nonabelian group of order 16 which is $B(5, 15)$, as shown by the following counterexamples. The definitions of the groups listed here are given near the end of Chapter 3.

- $D_8 \times C_2$ where $C_2 = \{1, x\}$

If we take the subset $S = \{a, b, ab, ax, bx\}$ and multiply in the usual manner, the products we get will be all sixteen elements of $D_8 \times C_2$. Therefore $D_8 \times C_2$ is not $B(5, 15)$.

- D_{16}

If we take the subset $S = \{a, b, ab, a^3, a^3b\}$, the products we get will be the sixteen elements of D_{16}. Therefore D_{16} is not $B(5, 15)$ and, in fact, it follows in a similar way as shown for $B(3, 7)$ groups that D_{2^n} is not $B(5, 15)$ for all $n \geq 4$.

- D_{16}^+

If we again take the subset $S = \{a, b, ab, a^3, a^3b\}$, the products we get will be the sixteen elements of D_{16}^+. Therefore D_{16}^+ is not $B(5, 15)$.

• $\underline{D_{16}^-}$

If we take the subset $S = \{a, b, ab, a^5, a^2b\}$, the products we get will be the sixteen elements of D_{16}^-. Therefore D_{16}^- is not $B(5, 15)$.

• $\underline{P = \langle a, b | a^4 = b^4 = 1, ba = a^3b \rangle}$

If we take the subset $S = \{a, b, ab, b^3, ab^2\}$, the products will be all sixteen elements of P. Therefore P is not $B(5, 15)$.

• $\underline{Q_{16} = \langle a, b | a^8 = 1, a^4 = b^2, ba = a^7b \rangle}$

If we take the subset $S = \{a, b, ab, a^5, a^5b\}$, the products will be the sixteen elements of Q_{16}. Therefore Q_{16} is not $B(5, 15)$.

• $\underline{H = \langle a, b | a^4 = b^4 = (ab)^2 = (a^2, b) = 1 \rangle}$

If we take the subset $S = \{a, b, ab, ab^2, ab^3\}$, the products will be all sixteen elements of H. Therefore H is not $B(5, 15)$.

• $\underline{D = \langle a, b, c | a^2 = b^2 = c^4 = 1, ac = ca, bc = cb, ba = c^2ab \rangle}$

If we take the subset $S = \{ca, cb, cab, b, c^2a\}$, the products will be the sixteen elements of D. Therefore D is not $B(5, 15)$.

We will also look at some more groups of small order > 16.

• $\underline{S_4}$

If we take the subset $S = \{(12), (34), (123), (1243), (1423)\}$, we get (at least) the sixteen products e (the identity permutation), (12)(34), (13), (143), (13)(24), (1234), (124), (14)(23), (23), (1243), (132), (1432), (1342), (243), (123), and (1324). Therefore S_4 is not $B(5, 15)$.

We will now go back and try some more possibilities involving the quaternion group of order 8.

• $Q_8 \times C_p$ where $C_p = \{1, x, \ldots, x^{p-1}\}$ and p is any integer with $p > 2$

If we take the subset $S = \{(a,1), (b,x), (ab,x), (a^3b,1), (a^3,x)\}$, we get (at least) the sixteen products $(a^2,1)$, (ab,x), (a^2b,x), $(b,1)$, $(1,x)$, (a^3b,x), (a^2,x^2), (a,x^2), (a^3,x), (ab,x^2), (b,x), (a^3,x^2), (a^2b,x^2), $(a^2b,1)$, (a,x), and (a^3b,x^2). Therefore $Q_8 \times C_p$ is not a $B(5,15)$ group.

• $Q_8 \times C_2 \times C_2$ where x and y are generators of different C_2's

If we take the subset $S = \{(a,1,1), (b,x,1), (ab,1,y), (a^3,1,y), (a^2b,1,y)\}$, we get (at least) the sixteen products $(a^2,1,1)$, $(ab,x,1)$, $(a^2b,1,y)$, $(1,1,y)$, $(a^3b,1,y)$, $(a^3b,x,1)$, (a,x,y), (ab,x,y), $(1,x,y)$, $(b,1,y)$, (a^3,x,y), $(a^2b,1,1)$, $(a,1,1)$, (a^3b,x,y), $(b,1,1)$, and $(ab,1,1)$. Therefore $Q_8 \times C_2 \times C_2$ is not a $B(5,15)$ group.

So we have shown that $G \cong Q_8 \times C_2$ is the only group of order 16 that is $B(5,15)$, and that S_4 and the dihedral 2-groups of order ≥ 16 are not $B(5,15)$. We have also shown that the only Hamiltonian group that satisfies the conditions for a nontrivial, nonabelian $B(5,15)$ group is $G \cong Q_8 \times C_2$. Although more work is still required, it is becoming reasonable to suggest that the only nontrivial, nonabelian $B(5,15)$ group is the Hamiltonian group $G = Q_8 \times C_2$.

Chapter 5

General Results

In this chapter, we will present the (very few) general results which are known about $B(n,k)$ groups. As mentioned in the introduction, we no longer insist that G be finite. The first result is an improved version of a theorem by Brailovsky [3].

Recall (Definition 1.2) that if $A = \{a_1, \ldots a_k\}$ is a k-subset of a group G, then $A^2 = \{a_i a_j | 1 \leq i, j \leq k\}$.

Theorem 5.1 *Let G be a group and let $k > 2$ be an integer such that $(k^3 - 2k + 1) < |G|/2$, if G is finite. Suppose that the condition $|A^2| \leq k(k+1)/2$ is satisfied by every k-subset $A \subseteq G$. Then G is abelian.*

To prove the theorem we first need to show that the following proposition holds when G satisfies the conditions of the theorem.

Proposition 5.1 *If $2 < \ell \leq k$ and $|B^2| \leq \frac{\ell(\ell+1)}{2}$ for all ℓ-subsets B of G, then $|A^2| \leq \frac{(\ell-1)\ell}{2}$ for all $\ell - 1$-subsets A of G.*

Proof: Let $A = \{a_1, a_2, \ldots, a_{\ell-1}\}$ be an $(\ell-1)$-subset of G. If we assume to the contrary that $|A^2| > \frac{(\ell-1)\ell}{2}$, then clearly $|A^2| \leq \frac{\ell(\ell+1)}{2} \leq \frac{k(k+1)}{2}$

We denote $K_1^A = \{x \in G | xA \cap A^2 \neq \emptyset\}$ and $K_2^A = \{x \in G | Ax \cap A^2 \neq \emptyset\}$. Note that $x \in K_1^A \Leftrightarrow xA \cap A^2 \neq \emptyset \Leftrightarrow xa_i = a_j a_k$ for some a_i, a_j, $a_k \Leftrightarrow x = a_j a_k a_i^{-1}$. We readily obtain that

$$|K_1^A| \leq |A^2| \cdot |A| \leq \frac{\ell(\ell+1)}{2}(\ell-1) = \frac{\ell^3 - \ell}{2}, \tag{5.1}$$

and similarly we get $|K_2^A| \leq \frac{\ell^3-\ell}{2}$, so

$$|K_1^A \cup K_2^A| \leq \ell^3 - \ell. \tag{5.2}$$

Here we note that $A \subseteq K_1^A$ and $A \subseteq K_2^A$, so at this point we are actually counting the elements of A twice in (5.2) above. We can now improve (5.2) to

$$|K_1^A \cup K_2^A| = |K_1^A| + |K_2^A| - |K_1^A \cap K_2^A| \leq \ell^3 - \ell - |A| = \ell^3 - \ell - (\ell-1) = \ell^3 - 2\ell + 1. \tag{5.3}$$

Since $|G| > 2(k^3 - 2k + 1) \geq 2(\ell^3 - 2\ell + 1)$, we can choose $y \notin K_1^A \cup K_2^A$ and let $C = A \cup \{y\}$. Since $y \notin A$, then $|C| = \ell$. Next, consider $C^2 = A^2 \cup Ay \cup yA \cup \{y^2\}$, then by our choice of y, we have $|A^2 \cup yA| = |A^2| + (\ell - 1)$. Furthermore, suppose that $yA \neq Ay$, then

$$|C^2| \geq |A^2| + (\ell-1) + 1 > \frac{(\ell-1)\ell}{2} + \ell = \frac{\ell(\ell+1)}{2}, \tag{5.4}$$

since Ay must have at least 1 element that is not in A^2 or yA. Hence, we have a contradiction. Therefore, we have shown that

$$yA = Ay \quad \forall y \in G \setminus \{K_1^A \cup K_2^A\}. \tag{5.5}$$

Next, we denote $N_G(A) = \{x \in G \mid xAx^{-1} = A\}$, called the normalizer of A in G. Obviously, $N_G(A)$ is a subgroup of G and, if we apply 5.3 and 5.5 above, $|G \setminus N_G(A)| \leq \ell^3 - 2\ell + 1$. If G is infinite, then $N_G(A) = G$ since $|G \setminus N_G(A)| < \infty$. On the other hand, if G is finite, then again $N_G(A) = G$, since $\frac{|G|}{2} > \ell^3 - 2\ell + 1$ by the condition of the theorem. It follows that $gAg^{-1} = A \ \forall g \in G$. In particular, we note that $a_iA = Aa_i$ for all $a_i \in A$, so $A^2 = \{a_ia_j | i \leq j\}$. It thus follows that (just as with abelian groups) $|A^2| \leq \frac{(\ell-1)\ell}{2}$, which is a contradiction. The proof of Proposition 5.1 is complete. □

We now finish the proof of Theorem 5.1.

Proof: (Theorem 5.1) Suppose that a nonabelian group G satisfies the condition of the theorem. It follows from Proposition 5.1 that $|A^2| \leq \frac{\ell(\ell+1)}{2}$ for any ℓ-element subset $A \subseteq G$, where $2 \leq \ell < k$. In particular, this holds for $\ell = 2$, which means that G is $B(2,3)$. Then, as shown in Theorem 2.1, $G = Q_8 \times C_2 \times \ldots \times C_2$. Since such a group G is not $B(3,6)$ by Theorem 3.1, we have a contradiction to the fact that the above condition also holds for $\ell = 3$. Thus G must be abelian and the theorem is proved. □

Theorem 5.1 above is an improvement of Brailovsky's bound on the order of G (from $\ell^3 - \ell$ down to $\ell - 2\ell + 1$) for which the conditions hold, but it seems hard to improve this bound further. If this were possible, it could be useful in finding which groups are $B(n,k)$ for some n and k. For example, we could find a finite list

of nonabelian groups that could be $B(5, 15)$, which would help us in formulating a theorem for that case. Unfortunately, even the improved bound is still too big to provide a list of practical length of nonabelian groups.

The next result was proved by Herzog, Longobardi and Maj [6].

Theorem 5.2 *The following are equivalent for a group G.*

(i) G is a $B(n, n^2 - 1)$ group for some integer n.

(ii) Either the subgroup of G generated by the squares of the elements of G is finite, or G contains a normal abelian subgroup of finite index on which each element of G acts by conjugation either as the identity automorphism or as the inverting automorphism.

We will only provide the proof for $(ii) \Rightarrow (i)$ here.

Proof: We note first that if a group G satisfies the first condition in (ii), then a large enough value of n will force any n-subset to have a repeated square. So we proceed with the second condition.

We are given that G contains a normal abelian subgroup H of index n, and that every element of G acts on H either as the inverting automorphism or the identity automorphism. So we have

$$G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n,$$

where $g_1, \ldots g_n \in G$. If we take an $(n + 1)$-subset A, then A must contain $h_1 g_i$ and $h_2 g_i$ for some i and $h_1, h_2 \in H$. Since we wish to show that A^2 contains a repeated

product, we must investigate two cases.

Case 1: The identity automorphism

We assume that g_i acts as the identity automorphism on H. So $h = g_i^{-1}hg_i \Rightarrow g_ih = hg_i$ for all $h \in H$. But then $(h_1g_i)(h_2g_i) = h_1h_2g_ig_i = h_2h_1g_ig_i = (h_2g_i)(h_1g_i)$, which gives a repeated product.

Case 2: The inverting automorphism

We assume that g_i acts as the inverting automorphism on H. So $h = g_i^{-1}h^{-1}g_i \Rightarrow g_ih = h^{-1}g_i$ for all $h \in H$. But then $(h_1g_i)^2 = h_1g_ih_1g_i = h_1h_1^{-1}g_i^2 = g_i^2$ and $(h_2g_i)^2 = h_2g_ih_2g_i = h_2h_2^{-1}g_i^2 = g_i^2$. So $(h_1a_i)^2 = (h_2a_i)^2$, giving a repeated product.

We get a repeated product in both cases, so G is $B(n+1,(n+1)^2-1)$, as required.

□

We note that an obvious example of a group satisfying the second condition in (ii) of Theorem 5.2 is a dihedral group of any order, even infinite. We can write any dihedral group G as $G = \langle a\rangle \cup \langle a\rangle b$, so, by the proof given above, any dihedral group is a $B(3,8)$ group.

We close with a small, new result about elementary abelian 2-groups.

Theorem 5.3 *If $G \cong C_2 \times \ldots \times C_2$ then G is a $B(k,\ell)$ group, where $\ell = \frac{(k-1)k}{2} + 1$.*

Proof:

If we take a k-subset of G, we will get at most $\frac{k(k+1)}{2}$ products, since G is abelian. But since $x^2 = 1$ for any $x \in G$, then k of these products will be equal to 1. So we

have at most

$$\frac{k(k+1)}{2} - k = \frac{k^2+k-2k}{2} = \frac{k^2-k}{2} = \frac{k(k-1)}{2}$$

products that are not equal to the identity, for a total of at most $\frac{k(k-1)}{2}+1 = \ell$ distinct products. So G must be $B(k,\ell)$, as required. $\square$

We note that if we have fewer than $k-1$ copies of C_2, then the bound ℓ in Theorem 5.3 can be improved.

Bibliography

[1] Bell, H. and Klein, A., *Combinatorial commutativity and finiteness conditions for rings*, Comm. Algebra **29** (2001), 2935-2943.

[2] Berkovich, Ja. G., Freiman, G. A. and Praeger, C. E., *Small squaring and cubing properties for finite groups*, Bull. Austral. Math. Soc. **44** (1991), 429-450.

[3] Brailovsky, L., *A characterization of abelian groups*, Proc. Amer. Math Soc. **117** (1993), 627-629.

[4] Freiman, G. A., *On two- and three-element subsets of groups*, Aequationes Math. **22** (1981), 140-152.

[5] Hall Jr., M., *The theory of groups*, The Macmillan Company, New York (1959), 190-192.

[6] Herzog, M., Longobardi, P. and Maj, M., *On a combinatorial problem in group theory*, Israel J. Math. **82** (1993), 329-340.

[7] Longobardi, P., and Maj, M., *The classification of groups with the small squaring property on 3-sets*, Bull. Austral. Math. Soc. **46** (1992), 263-269.

[8] Parmenter, M., *On groups with redundancy in multiplication*, Ars Combinatoria **63** (2002), 119-127.

[9] Rotman, J., *An introduction to the theory of groups*, Springer-Verlag, New York (1995).